Hacker Breaches Syscoin GitHub Account and Poisons Official Client

bleepingcomputer.com/news/security/hacker-breaches-syscoin-github-account-and-poisons-official-client/

Catalin Cimpanu

By
Catalin Cimpanu

- June 15, 2018
- 12:21 PM
- 0

A hacker gained access to the GitHub account of the Syscoin cryptocurrency and replaced the official Windows client with a version containing malware.

The poisoned Syscoin Windows client contained Arkei Stealer, a malware strain specialized in dumping and stealing passwords and wallet private keys. This malware is also detected as Trojan:Win32/Feury.B!cl.

Syscoin developers are now warning Syscoin users who downloaded version 3.0.4.1 of the Syscoin client between **June 09th, 2018 10:14 PM UTC** and **June 13th, 2018 10:23 PM UTC** that their systems might be infected with malware.

The affected files are (version number included in the file name is 3.0.4, but they install version 3.0.4.1):

syscoincore-3.0.4-win32-setup.exe
syscoincore-3.0.4-win64-setup.exe

Only Syscoin Windows client affected

Hackers only tampered with the Windows client and no other files available in the v3.0.4.1 release, which also included Mac and Linux clients, along with the adjacent source code.

The Syscoin clients are installed on an operating system and allow users to run a Syscoin node, which they can use to mine new Syscoin cryptocurrency or manage Syscoin funds.

The incident came to light yesterday when the Syscoin team received a warning from users that Windows Defender SmartScreen was marking downloads of the Syscoin Windows client as malicious.

What users need to do

After a thorough investigation of the report, the Syscoin team discovered that a hacker compromised one of its developers' GitHub accounts, and took actions to remove the malicious files and warn users.

All Windows users should identify their installation date:

- Right-click on syscoin-qt.exe in C:\Users[USERNAME]\AppData\Roaming\SyscoinCore or view in detailed list mode and make a note of the modified date.
- OR go to Settings->Apps and make a note of the installation date.

If the modified/installation date is between June 9th, 2018, and June 13th, 2018, take the following precautions:

- Backup any important data including wallets onto another storage medium outside of the affected computer. Treat this data cautiously as it may contain infectious code.
- Run an up-to-date virus scanner on your system to remove the threat.
- Passwords entered since the time of the infection should be changed from a separate device after ensuring the threat has been removed.
- Funds in unencrypted wallets or wallets that had been unlocked during the infection period, should be moved to a **newly generated** wallet on a secure computer.

Users who downloaded the Syscoin client between the above-mentioned interval but did not install it are advised to delete it and redownload a clean version.

While there are online guides with instructions on how to remove this particular malware strain, it's probably a better idea if users wiped and reinstalled the entire OS, just to be on the safe side.

The Syscoin team also announced that all of its developers with access to its GitHub account would also be forced to use two-factor authentication (2FA) and perform routine (file signature) checks of the files offered for download to detect similar incidents where hackers replace files in the future.

Related Articles:

Fake Binance NFT Mystery Box bots steal victim's crypto wallets

New powerful Prynt Stealer malware sells for just $100 per month

Beanstalk DeFi platform loses $182 million in flash-loan attack

Cryptocurrency DeFi platforms are now more targeted than ever

GitHub: Attackers stole login details of 100K npm user accounts

- Altcoin
- CryptoCurrency
- GitHub
- Hack
- Information Stealer

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

You may also like: